PATENTS • DESIGNS • COPYRIGHT • TRADE MARKS
The Patent Office

INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation and Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein together with the Statement of inventorship and of right to grant of a Patent (Form 7/77), which was subsequently filed.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

Dated 12th November 2001

#2

Patent
Attorney's Docket No. 032986-019

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	)	
	)	
Esa Turtiainen et al.	)	Group Art Unit: 2131
	)	
Application No.: 10/003,776	)	Examiner: Unassigned
	)	
Filed: November 15, 2001	)	Confirmation No.: 4500
	)	
For: Securing Voice over IP Traffic	)	

CLAIM FOR CONVENTION PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed:

Great Britain Patent Application No. 0028068.5

Filed: November 16, 2000

In support of this claim, enclosed is a certified copy of the prior foreign application. The prior foreign application was referred to in the oath or declaration. Acknowledgment of receipt of the certified copy is requested.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: JUNE 10, 2002

By: Michael J. Crowley
Registration No. 49,009

P.O. Box 1404
Alexandria, Virginia 22313-1404
(919) 941-9240

Patents Form 1/77

Patents Act 1977
(Rule 16)

The Patent Office

1/77

17NOV00 E584598-1 D01063
P01/7700 0.00-0028068.5

THE PATENT OFFICE
M
16 NOV 2000
RULE 97
NEWPORT

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office
Cardiff Road
Newport
South Wales
NP10 8QQ

1. Your reference — RL.P51317GB — 16 NOV 2000

2. Patent application number *(The Patent Office will fill in this part)* — 0028068.5

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

Telefonaktiebolaget LM Ericsson
SE-12625
Stockholm
Sweden

Patents ADP number *(if you know it)* — 76374800 2

If the applicant is a corporate body, give the country/state of its incorporation — SWEDEN

4. Title of the invention — Securing Voice over IP Traffic

5. Name of your agent *(if you have one)* — Marks & Clerk

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

Marks & Clerk
4220 Nash Court
Oxford Business Park South
Oxford
OX4 2RU

Patents ADP number *(if you know it)* — 727 1125 001

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day / month / year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*

a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

Yes

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	(none)
Description	7
Claim(s)	2
Abstract	1
Drawing(s)	3+3

10. If you are also filing any of the following, state how many against each item.

Priority documents	(none)
Translations of priority documents	(none)
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	1
Request for preliminary examination and search *(Patents Form 9/77)*	1
Request for substantive examination *(Patents Form 10/77)*	1
Any other documents *(please specify)*	(none)

11. I/We request the grant of a patent on the basis of this application.

Signature Marks & Clerk Date 15 November, 2000

Marks & Clerk

12. Name and daytime telephone number of person to contact in the United Kingdom: Dr. Robert Lind 01865 397900

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) If you need help to fill in this form or you have any questions, please contact the Patent Office on 08459 500505.

b) Write your answers in capital letters using black ink or you may type them.

c) If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.

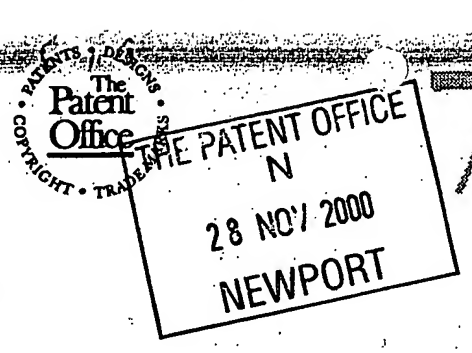
d) If you have answered 'Yes' Patents Form 7/77 will need to be filed.

e) Once you have filled in the form you must remember to sign and date it.

f) For details of the fee and ways to pay please contact the Patent Office.

Patents Form 7/77

Pa[illegible] Act 1977
(Rule 15)



7777

Statement of inventorship and of right to grant of a patent

The Patent Office

Cardiff Road
Newport
South Wales
NP10 8QQ

1. Your reference

RL.P51317GB

2. Patent application number
(if you know it)

3. Full name of the or of each applicant

Telefonaktiebolaget LM Ericsson

4. Title of the invention

SECURING VOICE OVER IP TRAFFIC

5. State how the applicant(s) derived the right from the inventor(s) to be granted a patent

By virtue of employment of the inventors

6. How many, if any, additional Patents Forms 7/77 are attached to this form?
(see note (c))

1

7. I/We believe that the person(s) named over the page *(and on any extra copies of this form)* is/are the inventor(s) of the invention which the above patent application relates to.

Signature: Marks & Clerk

Date: 24 November 2000

8. Name and daytime telephone number of person to contact in the United Kingdom

Dr. Robert Lind 01865 397900

Notes

a) *If you need help to fill in this form or you have any questions, please contact the Patent Office on 08459 500 505.*

b) *Write your answers in capital letters using black ink or you may type them.*

c) *If there are more than three inventors, please write the names and addresses of the other inventors on the back of another Patents Form 7/77 and attach it to this form.*

d) *When an application does not declare any priority, or declares priority from an earlier UK application, you must provide enough copies of this form so that the Patent Office can send one to each inventor who is not an applicant.*

e) *Once you have filled in the form you must remember to sign and date it.*

D 2

Enter the full names, addresses and postcodes of the inventors in the boxes and underline the surnames

Esa Turtiainen
Kartanonkuja 8 H
FIN-02360 Espoo
Finland

Patents ADP number *(if you know it)*: 116588600 1

Tommi Linnakangas
Piispantie 6 B 10
FIN-00370 Helsinki
Finland

Patents ADP number *(if you know it)*: 0116589400 1

(4)

Juha-Petri Kärnä
Hakarinne 2 0 186
02100 Espoo
Finland

0803637800 1.

Patents ADP number *(if you know it)*:

Reminder

Have you signed the form?

Patents Form 7/77

Patents Act 1977
(Rule 15)

7/77

Statement of inventorship and of right to grant of a patent

The Patent Office
Cardiff Road
Newport
South Wales
NP10 8QQ

1. Your reference

2. Patent application number
(if you know it)

3. Full name of the or of each applicant

4. Title of the invention

5. State how the applicant(s) derived the right from the inventor(s) to be granted a patent

6. How many, if any, additional Patents Forms 7/77 are attached to this form?
(see note (c))

7. I/We believe that the person(s) named over the page *(and on any extra copies of this form)* is/are the inventor(s) of the invention which the above patent application relates to.

Signature Date

8. Name and daytime telephone number of person to contact in the United Kingdom

Notes

a) If you need help to fill in this form or you have any questions, please contact the Patent Office on 08459 500 505.

b) Write your answers in capital letters using black ink or you may type them.

c) If there are more than three inventors, please write the names and addresses of the other inventors on the back of another Patents Form 7/77 and attach it to this form.

d) When an application does not declare any priority, or declares priority from an earlier UK application, you must provide enough copies of this form so that the Patent Office can send one to each inventor who is not an applicant.

e) Once you have filled in the form you must remember to sign and date it.

Enter the full names, addresses and postcodes of the inventors in the boxes and underline the surnames

Göran Schultz
Björkhagsgatan 10
21600 Pargas
Finland

Patents ADP number *(if you know it)*: 08031445001

Seppo Lindborg
Kuudestie 3
01510 Vantaa
Finland

Patents ADP number *(if you know it)*: 08031452001

08031452001

Patents ADP number *(if you know it)*:

Reminder

Have you signed the form?

Securing Voice over IP Traffic

Field of the Invention

The present invention relates to a method and apparatus for securing Voice over IP (VoIP) traffic.

Background to the Invention

There is an ever increasing demand for mobility in communications systems. However, this demand must be met in a manner which provides for the secure transfer of data between communicating parties. A concept known as the Virtual Private Network (VPN) has recently been introduced, with the aim of satisfying, by a combination of encryption and secure access, this demand. A VPN may involve one or more corporate Local Area Networks (LANs) or intranets, as well as users coupled to "foreign" LANs, the Internet, wireless mobile networks, etc.

An Internet Engineering Task Force (IETF) standard known as IPsec (RFC2401) has been defined and provides for the creation of a secure connection between parties in a VPN over IPv4 and IPv6. In the IPsec model the end points of the secure connection are identified by their IP addresses.

In order to allow IPSec packets to be properly encapsulated and decapsulated it is necessary to associate security services and a key between the traffic being transmitted and the remote node which is the intended recipient of the traffic. The construct used for this purpose is a "Security Association" (SA). SAs are negotiated between peer nodes using a mechanism known as "Internet Key Exchange" (IKE), and are allocated an identification known as a "Security Parameter Index" (SPI). The appropriate SA is identified to the receiving node by including the corresponding SPI in the headers of the transmitted data packets. Details of the existing SAs and the respective SPIs are maintained in a Security Association Database (SAD) which is associated with each IPSec node.

As already noted, IPSec SAs are negotiated using the IKE mechanism. More particularly, IPSec SAs make use of IKE phase 2. IKE phase 1 involves the negotiation of an IKE SA. When IKE phase 1 is initiated between two nodes, communications are carried out in the open. The mechanisms used must therefore be extremely secure and inevitably computationally intensive. At the end of phase 1 both nodes are authenticated to each other, and a shared secret is established between them. IKE phase 2 makes use of the IKE SA to negotiate one or more IPSec SAs. As the phase 2 negotiations are carried out using a secure mechanism, they can be much less computationally intensive than the phase 1 negotiation. Whilst a new IKE SA may be negotiated only infrequently (e.g. one a day or once a week), IPSec SAs may be negotiated every few minutes.

IPSec makes use of one or both of the Authentication Header (AH) and Encapsulation Security Payload (ESP) protocols which in turn make use of the corresponding established IPSec SA. Both of these protocols provide for the authentication of sent data packets whilst ESP provides in addition for the encryption of user data. The use of AH and/or ESP is agreed upon by the communicating nodes during the IKE negotiations.

The precise way in which IPSec is implemented in a system depends to a large extent upon the security policy of the organisation wishing to employ IPSec. For example, the organisation may specify end-points (e.g. user terminals) to which IP packets may be sent, or from which they may be received, the particular security levels to be used for encrypting packets, etc. Policy is stored in a Security Policy Database (SPD) which is also associated with each IPSec node. Typically, the SPD is distributed amongst a plurality of entities of the IPSec node.

It is expected that in the very near future IP networks will be used to carry significant volumes of voice data. The use of IP networks for real time voice communication is referred to as Voice over IP (VoIP). Indeed VoIP already exists, although in practice its applications are limited by the poor bandwidth and quality offered by current IP

standards and networks. As IP standards are revised and new standards created, it can be expected that more use will be made of VoIP.

The Internet is an open network in as much as unauthorised third parties can potentially intercept data and attempt to fraudulently transmit data. This is one of the main reasons for the creation of IPSec. Of course it is desirable to secure VoIP traffic and proposals have been made to allow the integration of VoIP with IPSec, such that VoIP traffic can be secured using the ESP protocol (which includes provision for data encryption). This solution is not without its problems however. The nature of speech and the real time transmission of speech requires the sending of relatively small data packets, containing in the region of 30-50 bits, with a high frequency. A typical ESP header, plus the ESP trailer (and authentication data) contains up to 160 bits, resulting in a doubling or trebling of the total packet size. This does not represent an efficient use of the IP resources. A similar problem applies to the transmission of other real time streamed data such as videoconferencing and multimedia data.

Summary of the Invention

The inventors of the present invention have recognised that, whilst IPSec does not represent an optimal solution for VoIP or other streamed data, it is likely to be installed on many terminals and devices employing streamed data. Certain components of IPSec may be advantageously employed with streamed data, providing that these components do not add excessively to the size of data packet.

According to a first aspect of the present invention there is provided a method of sending streamed data over an IP network from a first node to a second node, the method comprising:

using Internet Key Exchange (IKE) to establish an IKE security association (SA) between the first and second nodes;

encrypting the streamed data at the first node with a cipher using a shared secret forming part of said IKE SA or established using the IKE SA;

constructing IP datagrams containing in their payload segments of the encrypted streamed data, the datagrams not including an IPSec header or headers; and

sending the IP datagrams from the first node to the second node.

The present invention is particularly applicable to the secure transmission of VoIP data or videoconferencing data. It will be appreciated that such data does generally not require authentication as the data is self-authenticating. The main security concern is that of third parties monitoring the data, and this can be done by using IKE to generate an encryption key.

The method of the present invention may be carried out using an IKE process which forms part of an IPSec process. More particularly, the IKE process is defined by software and/or hardware components of an IPSec process. In this way, the invention does not require the provision of its own IKE components, but rather makes use of those of IPSec.

Preferably, the shared secret used to encrypt the streamed data is a secret forming part of an IPSec SA which is established by a negotiation between the peer nodes using the IKE SA. Alternatively however, the shared secret may form part of the IKE SA.

The method of the present invention may be used to secure streamed data sent between two nodes which represent end points for the data, e.g. two telephone terminals or PCs, or between two nodes which tunnel data between respective end points (e.g. gateways and firewalls).

According to a second aspect of the present invention there is provided apparatus for sending streamed data over an IP network to a peer node, the apparatus comprising:

processing means and memory containing software instructions for implementing IPSec protocols;

an application for delivering streamed data;

means for employing components of said processing means and memory containing software instructions for using Internet Key Exchange (IKE) to establish an

IKE security association (SA) between the first and second nodes, and to establish a shared secret between the first and second nodes using the IKE SA;

means for encrypting the streamed data with a cipher using the shared secret;

means for constructing IP datagrams containing in their payload segments of the encrypted streamed data, the datagrams not including an IPSec header or headers; and

transmission means for sending the IP datagrams from the first node to the second node.

The apparatus of the present invention may be an end user terminal such as a telephone, communicator, PDA or palmtop computer, or a personal computer (PC). Alternatively, the apparatus may be a firewall or gateway coupled to an end point which is the source of the streamed data.

Brief Description of the Drawings

Figure 1 illustrates schematically a Virtual Private Network (VPN) comprising an intranet;

Figure 2 illustrates at a general level the signalling between two nodes of the VPN of Figure 1 during a secure data connection establishment process;

Figure 3 illustrates at a more detailed level the signalling involved in an IKE phase 1 of the process of Figure 2;

Figure 4 illustrates a Quick Mode message exchange of an IKE phase 2 of the process of Figure 2; and

Figure 5 is a flow diagram illustrating a secure VoIP method according to an embodiment of the present invention.

Detailed Description of a Preferred Embodiment

The method which will now be described makes use of features described in the following documents: [IPsec] RFC 2401, Security Architecture for the Internet Protocol, November 1998; [REKEY] Internet Draft, IPsec Re-keying Issues; [IKE] RFC 2409, The Internet Key Exchange (IKE), November 1998; [ISAKMP] RFC 2408,

Internet Security Association and Key Management Protocol, November 1998; [INTDOI] RFC 2407, The Internet Security Domain of Interpretation for ISAKMP, November 1998. Reference should be made to these documents for a fuller understanding of the method.

Figure 1 illustrates a situation where a mobile wireless device 1 may use the Internet 2 to connect to an organisation's firewall or Security Gateway (SG) 3, and then to gain access to some correspondent host (e.g. a server or other machine) 4 connected to the organisation's intranet (i.e. corporate LAN) 5. An access network 6 couples the mobile host 1 to the Internet 2 via a gateway 7. The access network may be for example a GSM network using GPRS, or may be a third generation network such as a UMTS network. The Mobile device 1 includes hardware and software components for implementing IP, including IPSec. Using IKE (phase 1 and phase 2 as illustrated in Figure 2), the mobile terminal can create IPSec SAs with which it can securely exchange data with the correspondent host 4.

As has been explained above, IPSec results in large headers (and other components) being added to data packets and is therefore not suitable for VoIP traffic. In order to overcome this problem, the embodiment of the invention described here makes use only of the IKE component of IPSec.

Assuming that VoIP traffic is to be exchanged between the mobile device 1 (peer 1) and the correspondent host 4 (peer 2). Both peer nodes will make use of software applications which provides the interface to the user (this application may present a simulated telephone on the display of the correspondent host 4). A VoIP communication is initiated by one of the peer nodes sending a request to the other node. An IKE phase 1 negotiation is then carried out between the peers using ISAKMP - this is illustrated in Figure 3. The result of this negotiation is the authentication of the peers to one another, and the creation of an IKE (or ISAKMP) SA which defines amongst other things the encryption algorithm (to be used for negotiating IPSec SAs if required). The Phase 1 negotiation also results in the generation of a secret (or "key") which is shared between the two nodes.

The shared secret may be used to encrypt the VoIP data directly, using the encryption algorithm and other associated parameters associated with the IKE SA. In this case, the relevant encryption data is made available to the VoIP applications. However, rather than use the IKE SA data, it may be preferable to enter IKE phase 2 and negotiate a pair of IPSec SAs (one for each transmission direction). IKE phase 2 is illustrated in more detail in Figure 4. The IPSec SA data relevant to encryption, including a pair of encryption keys, is then passed to the VoIP applications. The advantage of using IKE phase 2 is that the IKE phase 1 negotiation need only be done occasionally, with IKE phase 2 being carried out each time a new connection is required.

Whichever SA is selected (IKE or IPSec), the VoIP application at the transmitting peer uses the encryption data to encrypt the streamed VoIP data generated by the application. The encrypted data is then passed to the TCP/IP layers for segmentation and encapsulation with standard IP headers. As the IP data is not subjected to the complete IPSec procedure, the resulting IP packets do not include IPSec headers including AH and ESP headers. At the receiving peer, the IP data packets are decapsulated and the reconstructed, encrypted data stream passed to the VoIP application for decryption. Figure 5 illustrates the interaction of the VoIP application at one of the peers with the IPSec and IP protocol layers ***(this is only my guess!)***.

Figure 6 is a flow diagram illustrating a method of setting up a VoIP connection between two peers.

It will be appreciated by the person of skill in the art that various modifications may be made to the above described embodiments without departing from the scope of the present invention. For example, in some circumstances security may only be required between the access network IP gateway 7 and the intranet IP gateway 3, in which case an IKE SA (and IPSec SA if necessary) will be negotiated between these nodes upon initiation of a VoIP communication by one of the end points 1,4. It is also envisaged that encryption may be used only between the device 1 and the intranet gateway 3 or between the access network gateway 7 and the correspondent host 4.

Claims

1. A method of sending streamed data over an IP network from a first node to a second node, the method comprising:

using Internet Key Exchange (IKE) to establish an IKE security association (SA) between the first and second nodes;

encrypting the streamed data at the first node with a cipher using a shared secret forming part of said IKE SA or established using the IKE SA;

constructing IP datagrams containing in their payload segments of the encrypted streamed data, the datagrams not including an IPSec header or headers; and

sending the IP datagrams from the first node to the second node.

2. A method according to claim 1, wherein said streamed data is VoIP data or videoconferencing data.

3. A method according to claim 1 or 2, wherein the method is carried out using an IKE process which forms part of an IPSec process.

4. A method according to claim 3, wherein the IKE process is defined by software and/or hardware components of an IPSec process

5. A method according to any one of the preceding claims, wherein the shared secret used to encrypt the streamed data is a secret forming part of an IPSec SA which is established by a negotiation between the peer nodes using the IKE SA.

6. A method according to any one of the preceding claims, wherein said peer nodes are end points for the data.

7. A method according to any one of claims 1 to 5, wherein said peer nodes tunnel data between respective end points.

8. Apparatus for sending streamed data over an IP network to a peer node, the apparatus comprising:

processing means and memory containing software instructions for implementing IPSec protocols;

an application for delivering streamed data;

means for employing components of said processing means and memory containing software instructions for using Internet Key Exchange (IKE) to establish an IKE security association (SA) between the first and second nodes, and to establish a shared secret between the first and second nodes using the IKE SA;

means for encrypting the streamed data with a cipher using the shared secret;

means for constructing IP datagrams containing in their payload segments of the encrypted streamed data, the datagrams not including an IPSec header or headers; and

transmission means for sending the IP datagrams from the first node to the second node.

8. Apparatus according to claim 8, the apparatus being an end user terminal such as a telephone, communicator, PDA or palmtop computer, or a personal computer (PC).

9. Apparatus according to claim 8, the apparatus being a firewall or gateway coupled to an end point which is the source of the streamed data.

ABSTRACT

Securing Voice over IP Traffic

A method of sending streamed data over an IP network from a first node 1 to a second node 4, the method comprising using Internet Key Exchange (IKE) to establish an IKE security association (SA) between the first and second nodes 1,4. A shared secret is established between the first and second nodes using the IKE SA, and the streamed data encrypted at the first node 1 with a cipher using the shared secret or a key derived using the shared secret. IP datagrams are constructed containing in their payload, segments of the encrypted streamed data, the datagrams not including an IPSec header or headers. The IP datagrams are then sent from the first node 1 to the second node 4.

Figure 1

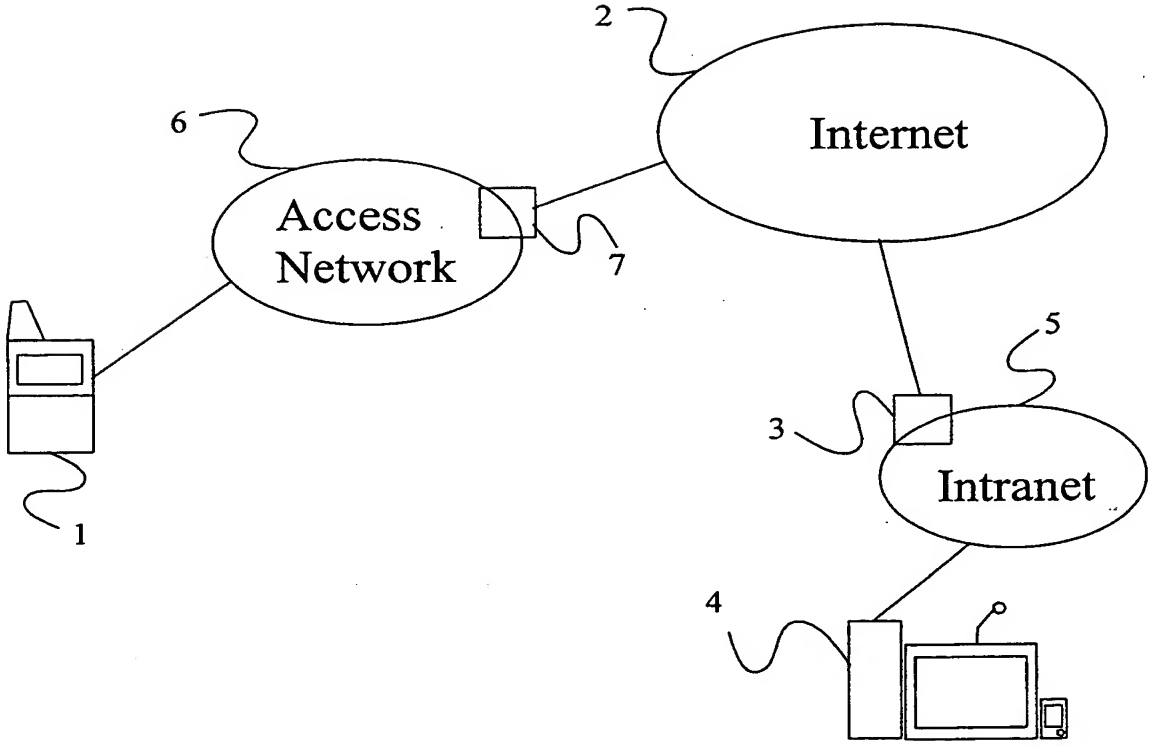


Figure 1

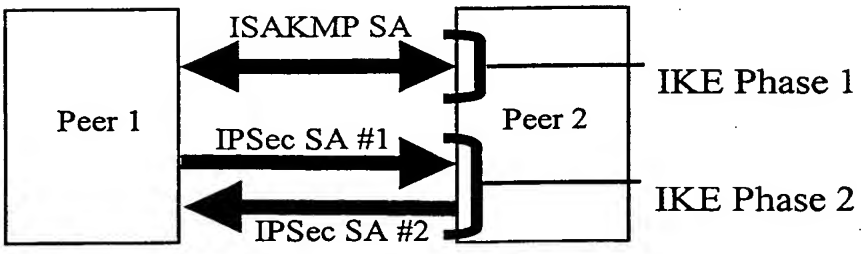


Figure 2

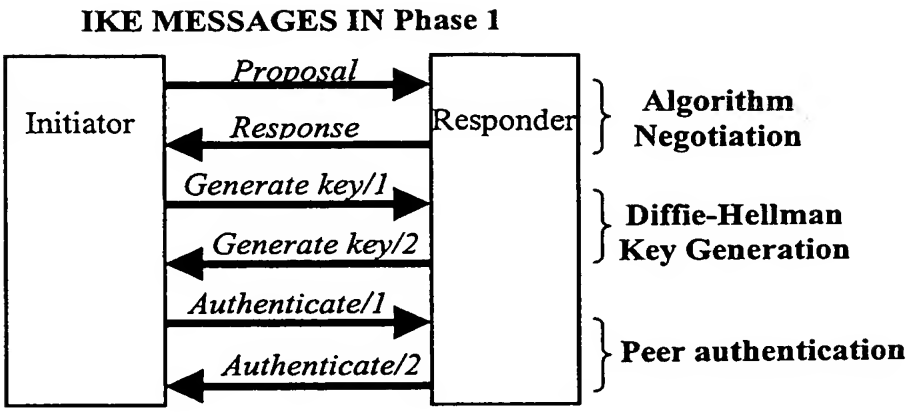


Figure 3

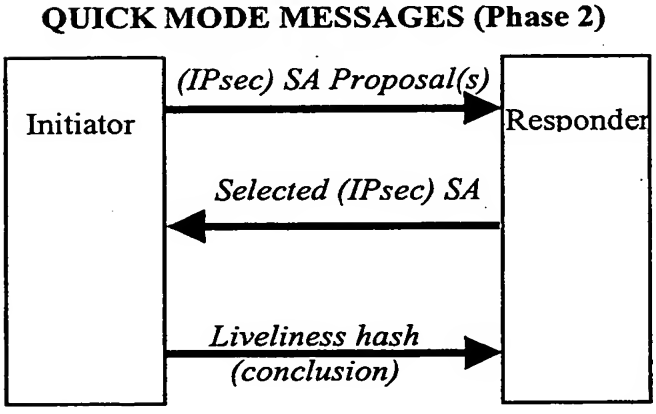


Figure 4

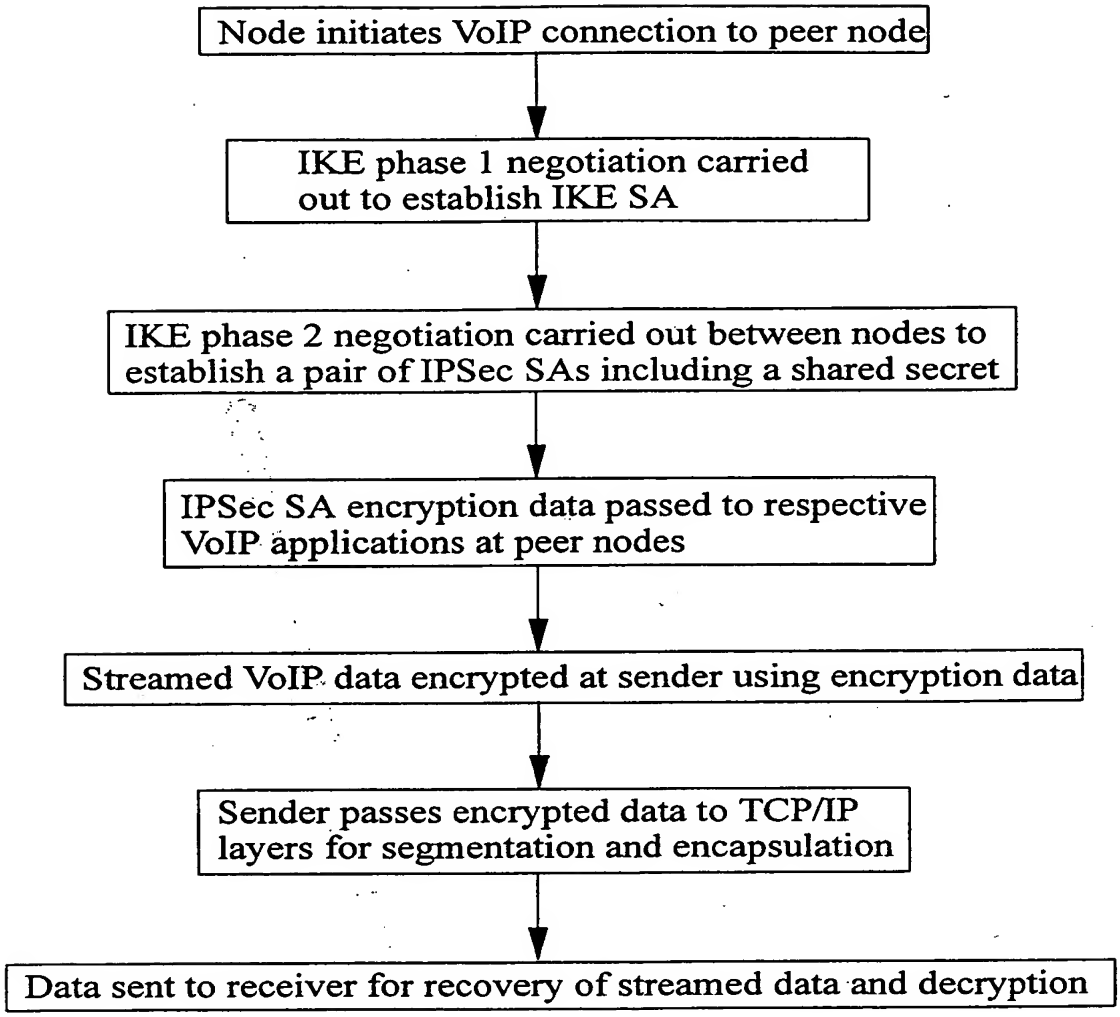

Node initiates VoIP connection to peer node
IKE phase 1 negotiation carried out to establish IKE SA
IKE phase 2 negotiation carried out between nodes to establish a pair of IPSec SAs including a shared secret
IPSec SA encryption data passed to respective VoIP applications at peer nodes
Streamed VoIP data encrypted at sender using encryption data
Sender passes encrypted data to TCP/IP layers for segmentation and encapsulation
Data sent to receiver for recovery of streamed data and decryption

Figure 5